PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: April 26, 1999

Application Number: Japanese Patent Application No. 11-118072

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE CORPORATION

August 30, 1999

Commissioner,
Patent Office Takeshi Isayama (Seal)

Certificate No.11-3060105

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:　１９９９年　４月２６日

出願番号
Application Number:　平成１１年特許願第１１８０７２号

出願人
Applicant (s):　日本電信電話株式会社

１９９９年　８月３０日

特許庁長官
Commissioner,
Patent Office　伊佐山建志

出証番号　出証特平１１－３０６０１０５

【書類名】　特許願

【整理番号】　NTTH107475

【提出日】　平成11年 4月26日

【あて先】　特許庁長官殿

【国際特許分類】　G06C

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　小川　宏

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　中村　高雄

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　富岡　淳樹

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　高嶋　洋一

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【選任した代理人】

【識別番号】　100100642

【弁理士】

【氏名又は名称】　稲垣　稔

【先の出願に基づく優先権主張】

【出願番号】　平成10年特許願第251193号

【出願日】　平成10年 9月 4日

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　抽出電子透かし情報統計処理方法、その装置及びプログラム記憶媒体

【特許請求の範囲】

【請求項１】　情報コンテンツに埋め込まれた電子透かし情報を再構成する方法において、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて、情報コンテンツに埋め込まれていた電子透かし情報を再構成することを特徴とする抽出電子透かし情報統計処理方法。

【請求項２】　請求項１記載の方法において、

抽出した電子透かし情報の信頼度のしきい値αを予め決めておき、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数からそのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求め、

情報コンテンツの透かし埋め込み対象領域から電子透かし情報の各ビットごとの電子透かし系列n_iを抽出し、

その抽出した電子透かし系列n_iに含まれるビット１又は０の数k_iを計算し、

ビット数k_iについて二項分布関数Ｆ（ｘ）を用いて出現確率Ｆ（k_i）を計算し、

Ｆ（k_i）＞αであればｉ番目の電子透かし情報w_iを１又は０に再構成し、

１－Ｆ（k_i）＞αであれば電子透かし情報w_iを０又は１に再構成し、

Ｆ（k_i）＞αでも、１－Ｆ（k_i）＞αでもなければ電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項３】　請求項２記載の方法において、

再構成した電子透かし情報w_iが１であればＦ（k_i）をその信頼度として出力し、

再構成した電子透かし情報w_iが０であれば１－Ｆ（k_i）をその信頼度として出力することを特徴とする抽出電子透かし情報統計処理方法。

【請求項４】　請求項１記載の方法において、

抽出した電子透かし情報の信頼度のしきい値αを決定しておき、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求め、

その二項分布関数Ｆ（ｘ）を用いて、その透かし系列が、透かし情報であるか否かを表わす確率を求め、

この確率がしきい値αを超えているか否かを調べ、超えていれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成し、

しきい値αを超えていなければ、電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項５】　請求項４記載の方法において、

上記再構成した電子透かし情報の信頼度として、上記確率を出力することを特徴とする抽出電子透かし情報統計処理方法。

【請求項６】　請求項１乃至５の何れかに記載の方法において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調することを特徴とする抽出電子透かし情報統計処理方法。

【請求項７】　請求項１記載の方法において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値αを決定しておき、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求めておき、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調されたものを復調し、

出現確率ｑを１／２とし、$0 \leqq F(x = x_0) \leqq 1 - \alpha$を満す最大の値$x_0$と

、$\alpha \leqq F(x=x_1) \leqq 1$を満す最小の値$x_1$とを求めておき、

ｉ番目に相当する電子透かし系列n_iに含まれるビット１又は０の数k_iを求め、

$k_i \leqq x_0$であればｉ番目の電子透かし情報w_iを０又は１に、$k_i \geqq x_1$であれば電子透かし情報w_iを１又は０にそれぞれ再構成することを特徴とする抽出電子透かし情報統計処理方法。

【請求項８】　請求項１記載の方法において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調し、

抽出した電子透かし情報の信頼度のしきい値αを決定しておき、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求めておき、

上記出現確率ｑを１／２とし、$0 \leqq F(x=x_0) \leqq 1-\alpha$又は$\alpha \leqq F(x=x_1) \leqq 1$を満す$x_0$又は$x_1$を求めておき、

透かし系列の二項分布の中心からのかたより度合の平均値がx_0以下又はx_1以上であるかを判定し、

x_0以下又はx_1以上であれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成し、

x_0以下又はx_1以上でなければ電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項９】　請求項８記載の方法において、

電子透かし情報を再構成した場合に、上記透かし系列の二項分布の中心からのかたより度合の平均値を、その再構成電子透かし情報の信頼度として出力することを特徴とする抽出電子透かし情報統計処理方法。

【請求項１０】　情報コンテンツに埋め込まれた電子透かし情報を再構成する方法において、

情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の出現確率の偏りから電子透かし情報を求めることを特徴とする抽出電子透かし情報統計処理方法。

【請求項１１】　情報コンテンツに埋め込まれた電子透かし情報を再構成する装置であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布関数Ｆ（ｘ）に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する抽出手段を有することを特徴とする抽出電子透かし情報統計処理装置。

【請求項１２】　請求項１０記載の装置において、

上記抽出手段は、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率と電子透かしの各ビットの繰り返し回数から二項分布関数Ｆ（ｘ）を求める手段と、

上記電子透かし情報の各ビット値ごとに電子透かし系列を抽出する手段と、

上記抽出した電子透かし系列の出現確率を、上記求めた二項分布関数Ｆ（ｘ）から求める手段と、

その求めた出現確率又は１－出現確率が信頼度のしきい値より大きいか否かを判定する手段と、

上記しきい値より大きいと判定された情報について電子透かし情報を再構成する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１３】　請求項１２記載の装置において、

上記求めた出現確率から、上記再構成した情報ビットについての信頼度を求めて、その再構成情報ビットと共に出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１４】　請求項１１記載の装置において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値αが決定されてあり、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）が求められてあり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する手段と、

上記抽出手段は、

ｉ番目に相当する電子透かし系列n_iに含まれるビット１又は０の数k_iを求める手段と、

出現確率ｑを１／２とし、$0 \leqq F(x=x_0) \leqq 1-\alpha$を満す最大の値$x_0$と$k_i$を比較し、$k_i \leqq x_0$であれば、ｉ番目の電子透かし情報$w_i$を０又は１に再構成し、$\alpha \leqq F(x=x_1) \leqq 1$を満す最小の値$x_1$と$k_i$を比較し、$k_i \geqq x_1$であればｉ番目の電子透かし情報$w_i$を１又は０に再構成する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１５】　請求項１１記載の装置において、

抽出した電子透かし情報の信頼度のしきい値αが決定されてあり、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求める手段と、

その二項分布関数Ｆ（ｘ）を用いて、その透かし系列が、透かし情報であるか否かを表わす確率を求める手段と、

この確率がしきい値αを超えているか否かを調べる判定手段と、

その判定手段でしきい値を超えていると判定されると、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する手段と、

上記判定手段でしきい値αを超えていないと判定されると、電子透かし無しもしくは不明と判定する手段とを備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１６】　請求項１５記載の装置において、

上記再構成した電子透かし情報の信頼度として、上記確率を出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１７】　請求項１１、１３、１５、１６の何れかに記載の装置において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１８】　請求項１１記載の装置において、

抽出した電子透かし情報の信頼度のしきい値αが決定されてあり、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）が求められてあり、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する手段と、

上記抽出手段は、

上記出現確率ｑを１／２とし、$0 \leqq F(x=x_0) \leqq 1-\alpha$ 又は $\alpha \leqq F(x=x_1) \leqq 1$ を満す x_0 又は x_1 と透かし系列の二項分布の中心からのかたより度合の平均値とを比較し、その平均値が x_0 以下又は x_1 以上であるかを判定する手段と、

その判定が x_0 以下又は x_1 以上であれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する手段と、

x_0 以下又は x_1 以上でなければ電子透かし無しもしくは不明と判定する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１９】　請求項１７記載の装置において、

電子透かし情報が再構成されると、上記透かし系列の二項分布の中心からのかたより度合の平均値を、その再構成電子透かし情報の信頼度として出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項２０】　情報コンテンツに埋め込まれた電子透かし情報を再構成す

るプログラムを格納した記憶媒体であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する処理を

コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項２１】　請求項２０記載の記憶媒体において、

抽出した電子透かし情報の信頼度のしきい値αが予め決められてあり、

上記電子透かし情報を再構成する処理は、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数からそのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求める処理と、

情報コンテンツの透かし埋め込み対象領域から電子透かし情報の各ビットごとの電子透かし系列n_iを抽出する処理と、

その抽出した電子透かし系列n_iに含まれるビット１又は０の数k_iを計算する処理と、

ビット数k_iについて二項分布関数Ｆ（ｘ）を用いて出現確率Ｆ（k_i）を計算する処理と、

Ｆ（k_i）＞αであればｉ番目の電子透かし情報w_iを１又は０に再構成する処理と、

１－Ｆ（k_i）＞αであれば電子透かし情報w_iを０又は１に再構成する処理と、

Ｆ（k_i）＞αでも、１－Ｆ（k_i）＞αでもなければ電子透かし無しもしくは不明と判定する処理とよりなることを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項２２】　請求項２１記載の記憶媒体において、

再構成した電子透かし情報w_iが１であればＦ（k_i）をその信頼度として出力し、

再構成した電子透かし情報w_iが０であれば１－Ｆ（k_i）をその信頼度とし

て出力する処理を上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項２３】　請求項２０記載の記憶媒体において、

抽出した電子透かし情報の信頼度のしきい値αが決定されてあり、

上記電子透かし情報を再構成する処理は、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求める処理と、

その二項分布関数Ｆ（ｘ）を用いて、その透かし系列が、透かし情報であるか否かを表わす確率を求める処理と、

この確率がしきい値αを超えているか否かを調べる処理と、

しきい値αを超えていれば、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する処理と、

しきい値αを超えていなければ、電子透かし無しもしくは不明と判定する処理とよりなることを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項２４】　請求項２３記載の記憶媒体において、

上記再構成した電子透かし情報の信頼度として、上記確率を出力する処理を上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項２５】　請求項２０乃至２４の何れかに記載の記憶媒体において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する処理を上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項２６】　請求項２０記載の記憶媒体において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値αが決定されてあり、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）が求められてあり、

上記電子透かし情報を再構成する処理は、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調されたものを復調しする処理と、

ｉ番目に相当する電子透かし系列n_iに含まれるビット１又は０の数k_iを求める処理と、

k_iが、出現確率ｑを１／２とし、$0 \leqq F(x = x_0) \leqq 1-\alpha$を満す最大の値$x_0$以下であればｉ番目の電子透かし情報$w_i$を０又は１に再構成する処理と、

k_iが、出現確率ｑを１／２とし、$\alpha \leqq F(x = x_1) \leqq 1$を満す最小の値$x_1$以上であれば電子透かし情報$w_i$を１又は０に再構成する処理とよりなることを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【請求項２７】　請求項２０記載の記憶媒体において、

上記情報コンテンツは、電子透かし情報として実際に埋め込まれた情報系列が、疑似乱数系列により変調されたものであり、

抽出した電子透かし情報の信頼度のしきい値αが決定されてあり、

情報コンテンツから任意に抽出した１ビット系列のビット１又は０の出現確率ｑと電子透かしの各ビットの繰り返し回数ｔから、そのビット系列に１又は０がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）が求められてあり、

上記出現確率ｑを１／２とし、$0 \leqq F(x = x_0) \leqq 1-\alpha$又は$\alpha \leqq F(x = x_1) \leqq 1$を満す$x_0$又は$x_1$が求められてあり、

電子透かし情報再構成処理前に疑似乱数系列で、上記変調された情報コンテンツを復調する処理と、

透かし系列の二項分布の中心からのかたより度合の平均値がx_0以下又はx_1以上であるかを判定する処理と、

x_0以下又はx_1以上と判定されると、情報コンテンツから読み取った透かし系列を多数決処理して電子透かし情報を再構成する処理と、

x_0 以下又は x_1 以上でないと判定されると電子透かし無しもしくは不明と判定する処理とを上記コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

マルチメディア著作物は、不正複製や改竄（かいざん）が容易であることから、情報利用者の正当な二次利用やコンテンツ提供者の情報発信の障害となっており、その著作権保護が訴えられている。画像や音声などのメディアの冗長性を利用し、人間に知覚されないように主情報である情報コンテンツに別の副情報を埋め込む技術に『電子透かし技術』がある。この技術は、重畳した情報の分離が困難なことより、マルチメディア著作物の著作権保護に有効な手段として考えられている。この発明は、電子透かしを用いたシステムにおける、抽出透かし情報の統計処理に関する方法及びその装置及び抽出情報の統計処理プログラムを格納した記憶媒体に関するものである。

【０００２】

【従来の技術】

特願平８－３０５３７０もしくは特願平８－３３８７６９もしくは特願平９－９８１２もしくは特願平９－１４３８８もしくは特願平９－５７５１６もしくは特願平９－１０９９２４もしくは特願平９－１６４４６６もしくは特願平９－１９７００３もしくは特願平９－２１８４６７もしくは特願平１０－３３２３９などに記載の電子透かし技術（Ｄｉｇｉｔａｌ　Ｗａｔｅｒｍａｒｋ，Ｄａｔａ　Ｈｉｄｉｎｇ，　Ｆｉｎｇｅｒ　Ｐｒｉｎｔｉｎｇ，　Ｓｔｅｇａｎｏｇｒａｐｈｙ，画像・音声深層暗号などとも呼ぶ）を用いたシステムにおいて一番重要な問題は、埋め込んだ情報の有無の判定および埋め込んだ情報の信頼性の精度である。電子透かしシステムは、電子透かしを埋め込んだ情報コンテンツに対する様々なメディア処理を想定して、情報コンテンツに埋め込まれている副情報（以下電子透かし情報と呼ぶことにする）がある程度壊れていても、正しい電子透かし情報を再構成する機構を持っているものが一般的である。しかしながら現状は、

再構成した透かし情報の正当性を定量評価できないものがほとんどであり、信頼性に欠けるものであった。

【０００３】

【発明が解決しようとする課題】

電子透かし情報を読みとった際に起こる問題である、電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価できる方法、装置、プログラム記憶媒体を提供することをこの発明は目的とする。

【０００４】

【課題を解決するための手段】

電子透かし処理は、電子透かし埋め込み・電子透かし抽出の対から成る。電子透かし埋め込み処理では、秘密鍵情報などを用いて、情報コンテンツ内の電子透かし対象領域Ａから電子透かし埋め込み領域Ｂ⊆Ａを選定し、固有の規則で領域Ｂ内のデータを変更する。電子透かし抽出処理では、電子透かし埋め込み領域Ｂのデータを解釈し、電子透かし情報を再構成する。この発明では、電子透かしが埋め込まれている情報コンテンツにおいて、この発明適用対象となる電子透かしアルゴリズムを用いて、電子透かし対象領域の全体であるＡから正誤を問わず任意の秘密鍵情報を用いて読みとられる電子透かし情報の統計学における二項分布をもとに、正しい秘密鍵情報を用いて透かし埋め込み領域Ｂから読みとられた電子透かし情報がどの程度確率的に起こり得るのかを判定する。

作用

この発明によれば、電子透かし技術において、情報コンテンツから読みとった透かし情報の信頼性を定量的に評価でき、電子透かしが入っていない情報コンテンツを有りと判断したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを読みとったりする確率を一定の値で抑えることができる。

【０００５】

【発明の実施の形態】

実施例１

予め意味が曖昧な言葉の定義を行なっておく。

電子透かし系列とは、情報コンテンツから読み出された再構成処理を行なう以前の情報系列を表し、電子透かし情報とは、情報コンテンツに本当に重畳したい、システムの運用上意味ある情報、もしくは、電子透かし系列を再構成処理し得られる情報を表すものとする。電子透かしの信頼度αとは、抽出した電子透かしの正当性を表す指標である。すなわち、抽出した電子透かしが、実際に画像に埋め込んでいた電子透かしと一致する確率である。逆に、電子透かしが埋め込まれていない画像から電子透かしを抽出したり、誤った電子透かし情報を抽出する確率を信頼度αを用いて２（１－α）と表現できる。

【０００６】

同様に埋め込み系列とは、実際に埋め込まれる情報を表し、埋め込み情報を変調したり、引き伸ばしたり、繰り返したりしている系列になっている。

以下にこの発明の実施例１を図面を参照して説明する。

図１は、この発明の背景となる電子透かしシステムの概要図である。

電子透かし情報１０１は、電子透かし埋め込み装置１０２によって情報コンテンツ１０３に埋め込まれ、電子透かし入り情報コンテンツ１０４に変換される。

【０００７】

電子透かし入り情報コンテンツ１０４は、無線・有線・パッケージ媒体などで流通する間に、情報圧縮やメディア処理などによって品質劣化した電子透かし入り情報コンテンツ１０５に変化する。

この発明の要部である電子透かし情報再構成装置１０６は電子透かし抽出装置１０７内部に実装され、電子透かし抽出装置１０７を用いて、劣化した電子透かし入り情報コンテンツ１０５から読みとった電子透かし系列を、電子透かし情報再構成装置１０６を用いて処理し、抽出電子透かし情報１０８を抽出するという構成になる。

【０００８】

以上が電子透かし埋め込み・抽出手順の概要である。

以下、電子透かし情報再構成処理の動作を詳細に説明する。

図２は、電子透かし抽出装置１０７の内部に実装された電子透かし情報再構成装置１０６の概要である。

電子透かし情報再構成装置１０６は、電子透かし抽出装置１０７を利用して、電子透かし情報の全埋め込み対象領域から任意の１ビット電子透かし系列を抽出したときにビット１が抽出される確率ｑを予め求めておく。

【０００９】

すなわち、１ビット電子透かし系列抽出処理部２０１のようなものを仮定し、電子透かし対象領域の全要素に対して１ビットずつ電子透かし系列の抽出を行ない（破線Ｌ１）、この全試行のうちビット１が何回取り出されたかの率を計算する。

この実施例ではビット１の抽出確率および個数を求めているが、ビット０の抽出確率および個数を求めても実装上の違いのみであり、本質的に変わらないことを留意しておく。

【００１０】

これより、電子透かしアルゴリズムを用いて、情報コンテンツ１０５の電子透かし対象領域から無作為に１ビット電子透かし系列の抽出を行なったときのビット０と１の出現確率はそれぞれ１－ｑおよびｑと計算される。

ｎビット電子透かし系列抽出処理装置２０２は、電子透かしが埋め込まれている情報コンテンツから電子透かしが埋め込まれたのべ回数だけ電子透かし系列の抽出を行なう。

【００１１】

ここで、電子透かし情報を$b_0\ b_1 \cdots b_{m-1}$，$b_i \in \{0, 1\}$，$i<m$（情報長ｍビット）、ｉビット目の電子透かし情報を情報コンテンツに埋め込んだ繰り返し回数（拡散率、ｃｈｉｐ－ｒａｔｅなどとも呼ぶ）をn_i回、読みとった電子透かし系列を

$$b'_{0,0}\ b'_{0,1} \cdots b'_{0,n0-1}\ b'_{1,0}\ b'_{1,1} \cdots b'_{1,n1-1} \cdots b'_{m-1,0}\ b'_{m-1,1} \cdots b'_{m-1,nm-1-1}$$

$$b'_{i,j} \in \{0, 1\}$$

（長さ$\Sigma_{r=0}^{m-1} n_r$ビット列）と定義する。

【００１２】

電子透かし情報再構成装置１０６は、ｎビット電子透かし情報抽出処理部２０

２から、電子透かし情報の０番目に相当する電子透かし系列の部分列からｍ－１番目に相当する電子透かし系列の部分列までを順次入力として受けとる（実線Ｌ２）。

次に、実際に電子透かし情報のｉビット目の電子透かし情報を再構成する方法を具体的に述べる。

【００１３】

電子透かし対象領域から任意にn_iビット電子透かし系列の抽出を行なったとき、このn_iビット列にビット１がｋ個現れる確率Ｐ（ｘ＝ｋ）は、二項分布の密度関数によって

$$P(x=k) = {}_{n_i}C_k \, q^k \cdot (1-q)^{ni-k} \qquad (1)$$

で表され、その分布関数Ｆ（ｘ）は、

$$F(x) = \sum_{k=0}^{x} {}_{n_i}C_k \, q^k \cdot (1-q)^{ni-k} \qquad (2)$$

$$(0 \leq x \leq n_i)$$

である。ただし、${}_{n_i}C_k$は、n_i個の中からｋ個のものを選ぶ組合せ数を表す。

【００１４】

電子透かし情報の信頼度のしきい値α（１／２＜α≦１）を設け、電子透かし情報再構成装置１０６に入力された電子透かし情報のｉ番目に相当する電子透かし系列の部分列$b'_{i,0}\ b'_{i,1} \cdots b'_{i,ni-1}$に含まれるビット１の数を

$$k_i = \sum_{r=0}^{ni-1} b'_{i,r}$$

によって計算し、式（２）を用いて電子透かし情報を

$$b_i = \begin{cases} 0 & 0 \leq F(k_i) \leq 1-\alpha \text{のとき} \\ 1 & \alpha \leq F(k_i) \leq 1 \text{のとき} \\ \text{不明もしくは無し} & 1-\alpha < F(k_i) < \alpha \text{のとき} \end{cases} \qquad (3)$$

と判定する。

【００１５】

見方を変えて電子透かし系列n_iに含まれるビット１の個数によって判定すると、$0 \leq F(x=x_0) \leq 1-\alpha$を満たす最大の$x_0$と、$\alpha \leq F(x=x_1) \leq 1$を満たす最小の$x_1$をしきい値として、図３に示すように$n_i$個中の１が$x_0$

以下なら０と、x_1 以上なら１と透かし情報を判定する。

図３の横軸は電子透かし系列に含まれるビット１の個数、縦軸はその出現頻度を表す。電子透かしが埋め込まれていない情報コンテンツではその任意に抽出したビット系列中に１が出現する頻度は二項分布となりその系列のビット数ｎの半分の所がピークとなる。しかし電子透かし情報が埋込まれた部分では電子透かし情報のビット０が埋め込まれた部分列n_i についてはビット１の出現頻度は、品質劣化がない場合は０であり、品質劣化があっても、小さな値、つまりx_0 以下であり、電子透かし情報のビット１が埋め込まれた部分列n_i についてはビット１の出現頻度は、品質劣化がない場合は、ｎ１であり、品質劣化があっても大きな値x_1 以上である。このように電子透かし情報が埋め込まれた電子透かし系列のビット１又は０の出現頻度は、二項分布に対し分布の中心が、偏よったものとなり、この発明ではこの偏よりを利用して電子透かし情報を、抽出した電子透かし系列から再構成する。

【００１６】

電子透かしシステムによっては、情報コンテンツ１０５から抽出された電子透かし系列の分布Ｐ（ｘ）の中心値に対する偏りから再構成した電子透かし情報を求め、抽出された電子透かし系列が統計的にどの程度の確率で出現するのかを式（２）の値で求めて、再構成された電子透かし情報が１の場合は$F(k_i)$を、情報が０の場合は$1-F(k_i)$を電子透かしの信頼度として付加して出力することも可能である。この電子透かしの信頼度$F(k_i)$，$1-F(k_i)$は、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求めたものになる。

【００１７】

この処理を電子透かし情報の情報長ｍビットに拡張した概念を図４に示す。

電子透かし情報再構成装置１０６は、再構成した電子透かし情報$b_0\ b_1 \cdots b_{m-1}$を抽出電子透かし情報１０８として出力する。

以上が電子透かし情報再構成処理の動作についてである。

この処理の手順を図５に示す。電子透かし入り情報コンテンツ１０５と、電子

透かし情報抽出に必要な秘密情報が入力され、その情報コンテンツ１０５と秘密情報とを用いて、各ビット値に関して、電子透かし系列を抽出する（Ｓ１）。透かしの信頼度のしきい値αを設定し（Ｓ２）、電子透かし情報のすべての埋め込み対象領域から透かしを任意に１ビット読み取ったときのビットが１である確率ｑを求める（Ｓ３）。この確率ｑと電子透かしの各ビットの繰り返し個数n_iとからビット系列に１がｘ個含まれる確率を表わす二項分布関数Ｆ（ｘ）を求める（Ｓ４）。

【００１８】

電子透かし系列の部分列を区別するｉを０とし（Ｓ５）、その部分列中のビットが１の個数$k_i = \Sigma_{j=0}^{ni-1} b'_{i,j}$を求め、その出現確率Ｆ（$k_i$）を求め、これが１－α以下であるかを調べる（Ｓ６）、Ｆ（k_i）≦１－αであれば電子透かし情報w'_iを０に再構成（Ｓ７）、ｉを＋１し（Ｓ８）、ｉ＜ｍならステップＳ６に戻る（Ｓ９）。ステップＳ６でＦ（k_i）≦１－αでなければＦ（k_i）≧αが成立するかを調べ（Ｓ１０）、成立すれば電子透かし情報w_iを１に再構成してステップＳ８に移る（Ｓ１１）。ステップＳ１０でＦ（k_i）≧αでなければ電子透かし無しもしくは不明と判定して処理を終了する（Ｓ１２）。ステップＳ９でｉがn_iより大となれば再構成された電子透かし系列｛w'_i｝を出力する。なおステップＳ１の各ビット値に関して電子透かし系列の抽出はステップＳ４とＳ５との間で行ってもよい。ステップＳ６，Ｓ１０でそれぞれ１－Ｆ（k_i）、Ｆ（k_i）がαより大であるかを判定している。

【００１９】

実施例１では、式（１）に表される分布に偏りがない、つまり、ｑ≒１／２となることを前提としている。

電子透かし情報のそれぞれのビット埋め込み回数n_iが、統計的特徴を得るのに十分な数である場合、一般的には、ｑ≒１／２となるが、ｑの値は、電子透かしアルゴリズムと情報コンテンツの特徴に依存するため、稀にｑが１／２から大きく外れた数となることがある。

【００２０】

この問題を回避する方法を実施例２で示す。

実施例２

以下にこの発明の実施例２を図面を参照して説明する。

図６は、この実施例２を付加した電子透かしシステムの概要図である。

電子透かし埋め込み装置１０２が情報コンテンツ１０３に電子透かし情報１０１を埋め込む際に、電子透かし情報の各ビット値をn_i回繰り返して埋め込む処理において、電子透かし埋め込み装置１０２の内部に実装された疑似乱数系列発生器（甲）５０１を用いて、埋め込み系列を変調し、これを情報コンテンツ１０３に埋め込む。

【００２１】

例えば、埋め込み系列を

$$b_{0,0}b_{0,1}\cdots b_{0,n0-1}b_{1,0}b_{1,1}\cdots b_{1,n1-1}\cdots b_{m-1,0}b_{m-1,1}\cdots b_{m-1,nm-1-1}$$

$$b_{i,j}\in\{0,\ 1\}$$

疑似乱数系列を

$$r_{i,0}\ r_{i,1}\cdots r_{i,ni-1}$$

$$r_{i,j}\in\{0,\ 1\}$$

とおくと、埋め込み系列を疑似乱数系列によって

$$m_{i,0}\ m_{i,1}\cdots m_{i,ni-1}$$

$$m_{i,j}=b_{i,j}\ (+)\ r_{i,j}$$

に変調する。Ａ（＋）ＢはＡとＢの排他的論理和を表わす。

【００２２】

この処理により、電子透かし抽出処理には、電子透かし系列埋め込みに用いたのと同じ疑似乱数系列が必要となる。

例えば、疑似乱数系列としてＭ系列を用いたとする。

すると、任意のＭ系列を用いて１ビット電子透かし系列抽出を行なったとき$q\simeq 1/2$となり、電子透かしアルゴリズムと情報コンテンツに依存することなくこの発明を適用可能となる。

【００２３】

電子透かし抽出では、電子透かし抽出装置１０７の内部に実装された疑似乱数系列発生器（乙）５０２を用いて、

$$b'_{i,j} = m_{i,j} \ (+) \ r_{i,j}$$

により復調する。

ここで、疑似乱数発生器（甲）５０１と疑似乱数発生器（乙）５０２は、同じ疑似乱数系列を発生するように実装する必要がある。

【００２４】

復調処理により得られた電子透かし系列

$$b'_{0,0}\ b'_{0,1} \cdots b'_{0,n0-1}\ b'_{1,0}\ b'_{1,1} \cdots b'_{1,n1-1} \cdots$$
$$b'_{m-1,0}\ b'_{m-1,1} \cdots b'_{m-1,nm-1-1}$$
$$b'_{i,j} \in \{0, 1\}$$

に対して、実施例１で説明した方法により電子透かし情報を再構成する。

【００２５】

読みとった電子透かし系列のビット１の出現確率ｑは、変調の有無に関わらず二項分布に近似できると考えられるため、この実施例で示した変調処理による密度関数の分布（１）への影響はない。

また、実装において、ｑ＝１／２と仮定できるため、つまりｑを求める処理（２０１）を行うことなく、式（２）でｑ＝１／２として計算することにより、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、高速化が図れる。

実施例３

実施例３では、実施例１および実施例２で示した発明の例に基づき、実際に数値を示して例を説明する。ここでは電子透かし情報を１ビットとし、その埋め込み繰り返し回数ｎを１２７回とし、電子透かし情報の全埋め込み対象領域から任意の１ビット電子透かし系列を抽出したときにビット１が抽出される確率ｑを１／２とする。信頼性のしきい値αを０．９９９９９（９９．９９９％の意）とすると、図３におけるx_0は３６、x_1は９０である。すなわち、以上の条件の下でこの発明は、電子透かし情報を、電子透かし系列（ｎビット）に現れる１の個数が３６以下である場合はビット０、９０以上の場合はビット１、それ以外の場合は電子透かしが不明もしくは無しと判定する。電子透かし情報有りと判定した場合、その正当率は９９．９９９％以上を保証できる。

実施例４

図５に示した実施例ではその処理手順から理解されるように、電子透かし情報の１ビットでも信頼性が得られない、つまりＦ（k_i）又は１－Ｆ（k_i）がαより小さなものになれば電子透かしなし、又は不明となり、電子透かし情報の再構成は不能となる。この実施例４はこのような問題を解決したものである。この場合は電子透かし情報の各ビットの埋め込み繰り返し回数は同一値ｎとする。

【００２６】

以下、情報コンテンツから読み取られた透かし系列$b'_{0,0}$，$b'_{0,1}$，…，$b'_{0,n-1}$，$b'_{1,0}$，$b'_{1,1}$，…，$b'_{1,n-1}$，$b'_{m,0}$，$b'_{m,1}$，…，$b'_{m,n-1}$から透かし情報w_0，w_1，…，w_{m-1}を再構成する方法を詳細に述べる（図７参照）。

Ｓｔｅｐ１．まず情報コンテンツと電子透かし情報抽出に必要な秘密情報とから各ビット値に関して電子透かし系列を抽出する。

【００２７】

Ｓｔｅｐ２．透かし情報の信頼度のしきい値α（１／２＜α≦１）を設定する。例えば、抽出した透かしの信頼度を９９％以上に設定したい場合は、α＝０．９９とする。

Ｓｔｅｐ３．電子透かし情報のすべての埋め込み対象領域から透かし系列を任意に１ビット読み取ったときに、それがビット‘１’である確率ｑを予め求める。すなわち、電子透かし抽出対象から無作為に電子透かし系列の抽出を行なったときのビット‘０’と‘１’の出現確率は１－ｑおよびｑと計算される。

【００２８】

Ｓｔｅｐ４．透かしの各ビット情報を構成する透かし系列にビット‘１’がｘ個含まれる確率は、二項分布関数Ｆ（ｘ）を用いて、

$$F(x)=\Sigma_{j=0}^{x}\ {}_nC_j\ q^j\cdot(1-q)^{n-j}$$

と表せる。

Ｓｔｅｐ５．ｎビットの透かし系列について、電子透かし情報であるかを表す確率がしきい値αを超えているか、つまり下記の式（４）を満すかを調べる。

【００２９】

【数１】

$$F\left(\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b'_{i,j}-\frac{n}{2}\right|}{m}+\frac{n}{2}\right)\geq\alpha \qquad \cdots\cdots(4)$$

なお｜ａ｜はａの絶対値を表わす。$\Sigma_{j=0}^{n-1} b_{i,j}$ －ｎ／２はそのｎビットの透かし系列の１ビットの個数の二項分布の中心からの偏よりを表わし、その$\Sigma_{i=0}^{m-1}$をｍで割ることは、全電子透かし情報のｍビットについての平均であり、ｎ／２は二項分布の中心である。

【００３０】

この式（４）がαより大であれば、透かし有りであり、よって各ｎビットの透かし系列のｍ個についてそれぞれ多数決処理により電子透かし情報を再構成すればよい。

【００３１】

Ｓｔｅｐ６．つまり、透かし有りと判定されると、すべての$0\leq i<m$に対して、

$\Sigma_{j=0}^{n-1} b_{i,j}$ ＜ｎ／２のとき：$w'_i=0$

$\Sigma_{j=0}^{n-1} b_{i,j}$ ≧ｎ／２のとき：$w'_i=1$

により透かし情報を再構成する。図の中７Ｓ６－１～Ｓ６－７によりこの処理が行われる。

Ｓｔｅｐ７．

【００３２】

【数２】

$$F\left(\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b_{i,j}-\frac{n}{2}\right|}{m}+\frac{n}{2}\right)<\alpha$$

のとき、透かし無しもしくは不明と判定する。ただし、｜ｘ｜はｘの絶対値を表

す。

透かしがあるかの判定式としては式（４）の代りに次の式（５）を用いてもよい。

【００３３】

【数３】

$$F\left(\frac{n}{2}-\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b'_{i,j}-\frac{n}{2}\right|}{m}\right)\leq 1-\alpha \qquad \cdots\cdots(5)$$

式（５）の左辺が１－αより大きければ透かし無しもしくは不明と判定する。

この実施例４では以上の説明から明らかなように、式（４）又は式（５）により、電子透かし情報系列の全体について統計的処理して透かしの有無を判定し、透かしありと判定されると、多数決処理により再構成を行うため、１ビットでも信頼度が小さいものが存在するために、電子透かし情報の再構成が不能になるようなことはない。

【００３４】

図７において、ステップＳ１の電子透かし系列抽出を、ステップＳ４とＳ５の間で行ってもよい。

この実施例４についても、実施例２で述べたように、電子透かし埋め込み系列に対し、疑似乱数系列で変調して情報コンテンツに対する埋め込みを行い、情報再構成する際に、取り出した透かし系列に対し、疑似乱数系列で復調し、その復調した系列について、式（４）の判定を行い、その結果αより大で透かしありと判定されると、復調系列に対し、実施例４のＳｔｅｐ６と同様な処理、つまり多数決処理により再構成を行うようにすることもできる。この全体の処理手順を図８に図７と対応する部分に同一符号を付けて示す。この例ではまず鍵情報Ｋｅｙから疑似乱数系列｛$r_{i,j}$｝を生成してステップＳ２に移る（Ｓ８）、またステップＳ４の次に電子透かし系列に対し疑似乱数系列｛$r_{i,j}$｝で復調を行ってステップＳ５へ移る（Ｓ９）。ステップＳ５の判定式（４）中の透かしビットｂ′

$_{i,j}$ はステップＳ９で復調したものであり、同様にステップＳ６での多数決処理もステップＳ９で復調したｂ′$_{i,j}$ について行う。

実施例５

疑似乱数系列によって透かし情報を拡散しているため、ｑを１／２に近似すると、透かし系列が透かしありか否かの判定を次のようにすることもできる。

【００３５】

電子透かしの各ビット情報を構成するｎビットの透かし系列にビット‘1’がｘ個含まれる確率は、二項分布関数Ｆ（ｘ）を用いて、

$$F(x)=\Sigma_{j=0}^{x}\ {}_nC_j\ (1/2^n)$$

と表せる。これより予め、

$$F(x=x_1)\geq\alpha$$

を満たす最小の整数x_1 を求めておくことにより、実施例４のＳｔｅｐ５．を透かし系列を疑似乱数系列で復調した系列について下記式（６）で判定できる。この場合は多数決判定と同程度の計算量に軽減することが可能である。

【００３６】

【数４】

$$\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b'_{i,j}-\frac{n}{2}\right|}{m}+\frac{n}{2}\geq x_1 \qquad \cdots\cdots(6)$$

この判定は透かし系列の二項分布の中心ｎ／２からの偏より度合の平均がx_1 以上であるかを判定していることになる。

式（６）が成立して透かし有りと判定されると、すべての$0\leq i<m$について、透かし系列を疑似乱数系列で復調したものを、下記のように多数決処理して、

$\Sigma_{j=0}^{n-1}\ b'_{i,j}<n/2$のとき：$w'_i=0$

$\Sigma_{j=0}^{n-1}\ b'_{i,j}>n/2$のとき：$w'_i=1$

透かし情報を再構成する。また、

【００３７】

【数５】

$$\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1} b'_{i,j}-\frac{n}{2}\right|}{m}+\frac{n}{2}<x_1$$

のときは、透かし無しもしくは不明と判定する。

Ｆ（ｘ＝x_1）≧αを満す最小の整数x_1を用いる代りに、Ｆ（ｘ＝x_0）≦１－αを満す最大の整数x_0を求めて処理してもよい。この場合の透かしがあるかの判定式は下記の式（７）となる。

【００３８】

【数６】

$$\frac{n}{2}-\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1} b'_{i,j}-\frac{n}{2}\right|}{m}\leq x_0 \qquad \cdots\cdots(7)$$

この式の左辺がx_0より大きければ透かし無し又は不明と判定する。

実施例６

式（４）により透かしありと判定した場合に、前記多数決処理により電子透かし情報を再構成すると共に、その再構成された透かし情報の系列の全体についての信頼度として、

【００３９】

【数７】

$$F\left(\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1} b'_{i,j}-\frac{n}{2}\right|}{m}+\frac{n}{2}\right)$$

を計算して出力する。

同様に式（５）により透かしありと判定した場合で、電子透かし情報を再構成

した場合は、その透かし情報の系列の全体についての信頼度として

【００４０】

【数８】

$$F\left(\frac{n}{2}-\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b'_{i,j}-\frac{n}{2}\right|}{m}\right)$$

を計算して出力する。

また式（６）により透かしありと判定した場合に、前記した多数決処理により電子透かし情報を再構成すると共にその透かし情報の系列の全体についての信頼度として、

【００４１】

【数９】

$$F\left(\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b'_{i,j}-\frac{n}{2}\right|}{m}+\frac{n}{2}\right)$$

を計算して出力する。

同様に式（７）により透かしありと判定した場合は、その透かし情報の系列の全体についての信頼度として

【００４２】

【数１０】

$$F\left(\frac{n}{2}-\frac{\sum_{i=0}^{m-1}\left|\sum_{j=0}^{n-1}b'_{i,j}-\frac{n}{2}\right|}{m}\right)$$

を計算して出力する。

実施例１乃至６においてビット１の抽出確率および個数を用いたが、ビット０の抽出確率および個数を用いても実装上の違いのみで、本質的に変わらない。

以下は実験例を示す。

【００４３】

実験対象画像として１２８×１２８画素の“ｌｅｎａ”画像を用い、信頼度のしきい値αを０．９９９９９９として実験を行なった。

実験１

１ビットの透かし情報“１”を秘密鍵情報“５０，０００”を用いて１２７回繰り返し埋め込み、任意の秘密鍵情報を用いて透かし系列の読みとりを行なった。図９は、秘密鍵情報に対する読みとり透かし系列のビット１の個数を示したものである。縦軸は読みとった透かし系列におけるビット１の個数、横軸は秘密鍵情報の値を表している。ただし、透かし対象領域Ａのビット１の出現頻度はｑ＝０．４９２２４７であった。正しい秘密鍵（５０，０００）を用いた場合、ビット１の個数が透かし有無の判定しきい値x_1より大きいことから、正当率９９．９９９９％で透かし情報は１であると判定でき、正しくない秘密鍵を用いた場合はすべて透かし無しもしくは不明と判定した。

実験２

７段のＭ系列（初期状態６４）を用いて変調した透かし系列を埋め込み、任意の秘密鍵情報と初期状態が任意のＭ系列を用いて実験１と同様の実験を行なった（図１０）。変調を行なうことにより、実験１のデータと比較してｑの値は０．５００００に、分散は３１．００８２６５から３１．７１８７７７とほとんど変化しなかった。透かしが抽出できたのは、正しい秘密鍵情報と疑似乱数系列の組を用いたときのみであった。また、透かし対象領域Ａの半分のデータに透かし系列を埋め込んだ場合、変調なしではｑ＝０．７４１５４７であったのに対し、変調を行なうことでｑ＝０．４９９７６８という結果が得られた。

【００４４】

【発明の効果】

１．統計学における二項分布に基づき電子透かし情報を判定することにより以下の効果がある。

－電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確

率を定量的に評価でき、その値を電子透かしの信頼度のしきい値αを用いて２（１－α）で抑えることができる。

【００４５】

２．電子透かし情報を埋め込む前に疑似乱数系列で変調することにより以下の効果がある。

－電子透かし情報の全埋め込み対象領域から任意の１ビット電子透かし系列を抽出したときにビット１が抽出される確率ｑの偏りを無くした。

－電子透かし抽出に必要な正しい電子透かしの秘密鍵情報と抽出した電子透かし系列を復調するのに必要な疑似乱数系列無しにｑの偏りから電子透かしの有無ならびにその値を検知することが困難となった。これは電子透かしシステムで重要な要素であるセキュリティの強化につながることである。

【００４６】

－実装において、ｑ＝１／２と仮定できるため、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、処理の高速化が図れる。

αは、抽出した情報の正当率の下限を示す指標であり、電子透かしシステムの内部で管理可能な情報となっている。これは、従来の電子透かしシステムに見られた、抽出した電子透かし情報の正当率を利用者に提示するものより優れている。

【００４７】

実施例１では、透かし情報｛w'_i｝を構成するビット情報のうち１ビットでも信頼度が低いものがある場合、透かし情報無しもしくは不明と判定する。しかしながら、このような場合でも、実施例４～６では透かし系列｛$b'_{i,j}$｝，（$0 \leq i < m$，$0 \leq j < n$）全体を統計的に見ると、透かし情報を十分再構成することができる場合が多いことから、透かし情報の有無を判定する式を改良し、透かし情報の全体を統計的処理をしたものとすることにより、透かし情報を構成するビット情報のうち数ビット信頼性が低いビットがある場合にでも、透かし情報の信頼性を定量的に評価し、その値を２（１－α）で押えることができ、かつ透かし情報を再構成することができる。また、実施例１では電子透かし系列から電子透かし情報を再構成するのに、すべてのｉに対して二項分布の分布関数Ｆ（ｘ

）を用いて、Ｆ（$\Sigma_{j=0}^{n-1} b'_{i,j}$）の値を計算する必要があったが、実施例４～６では分布関数を用いた計算を１回にすることができ、透かしの再構成にかかる計算量を軽減できる。

【００４８】

この発明は、誤り訂正符号と併用することでさらに大きな効果が得られる。すなわち、電子透かし情報の一部のビットだけが集中して壊れているような場合、抽出した情報は、一部のビットだけが不明で、それ以外のビット情報は正当性が高い状態にあると正確に判定できる。よって壊れたビット情報のみを誤り訂正することにより、確実に正しい情報が抽出できる。

【図面の簡単な説明】

【図１】

電子透かしシステムの概要を示す図。

【図２】

図１中の電子透かし抽出装置概要を示す図。

【図３】

電子透かし情報の判定を示す図。

【図４】

電子透かし情報再構成の概念を示す図。

【図５】

電子透かし抽出処理の手順を示す図。

【図６】

この発明の第２実施例の概要を示す図。

【図７】

この発明の第４実施例の処理手順を示す流れ図。

【図８】

この発明の第４実施例に対し、疑似乱数変調透かし情報の埋め込みを対象とした場合の処理手順を示す流れ図。

【図９】

透かし系列読みとり結果（変調なし）を示す図。

【図１０】

透かし系列読みとり結果（変調あり）を示す図。

【書類名】　図面

【図１】

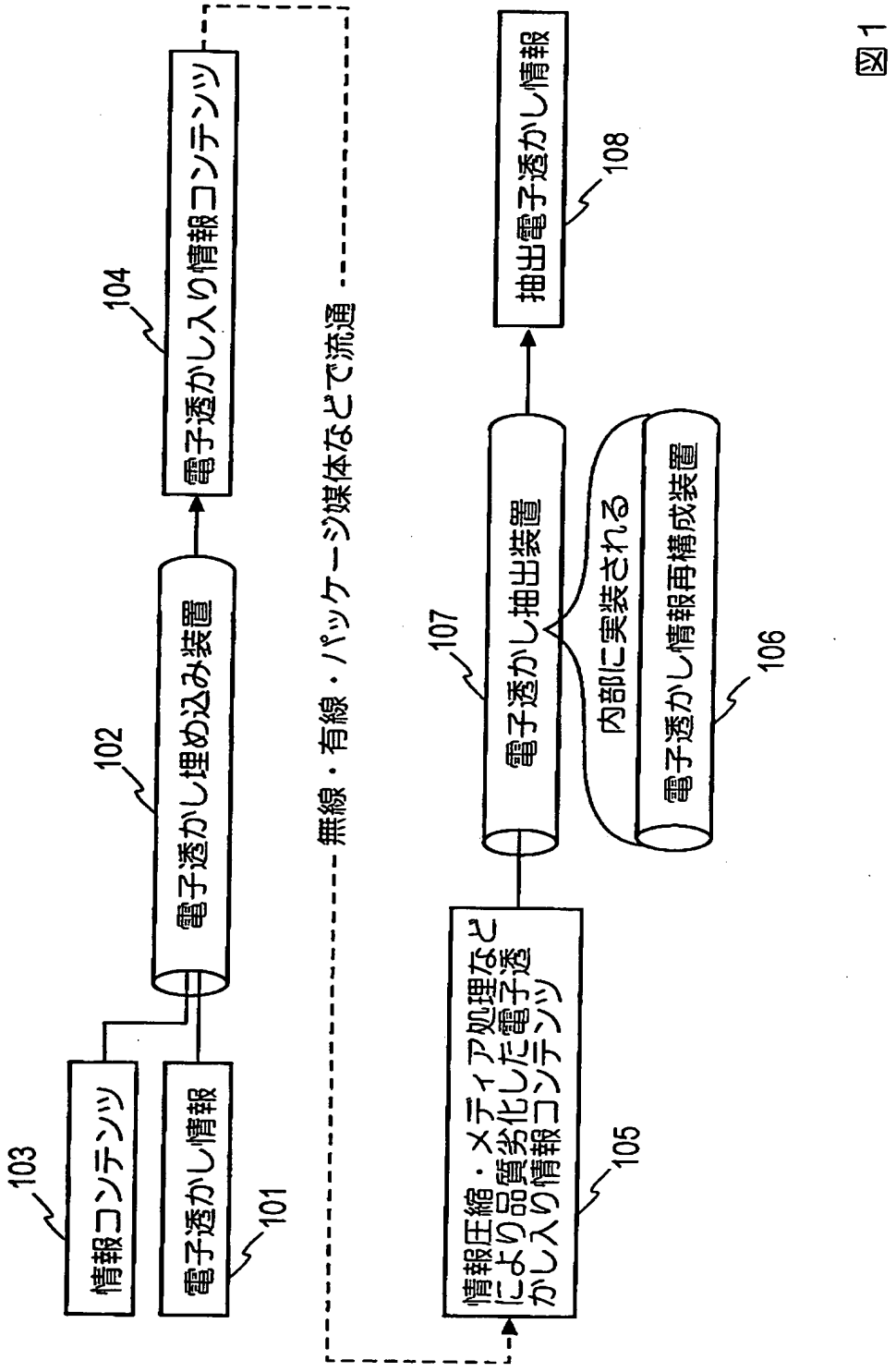
情報コンテンツ
電子透かし情報
電子透かし埋め込み装置
電子透かし入り情報コンテンツ
無線・有線・パッケージ媒体などで流通
情報圧縮・メディア処理などにより品質劣化した電子透かし入り情報コンテンツ
電子透かし抽出装置
抽出電子透かし情報
内部に実装される
電子透かし情報再構成装置
101
102
103
104
105
106
107
108

図１

【図２】

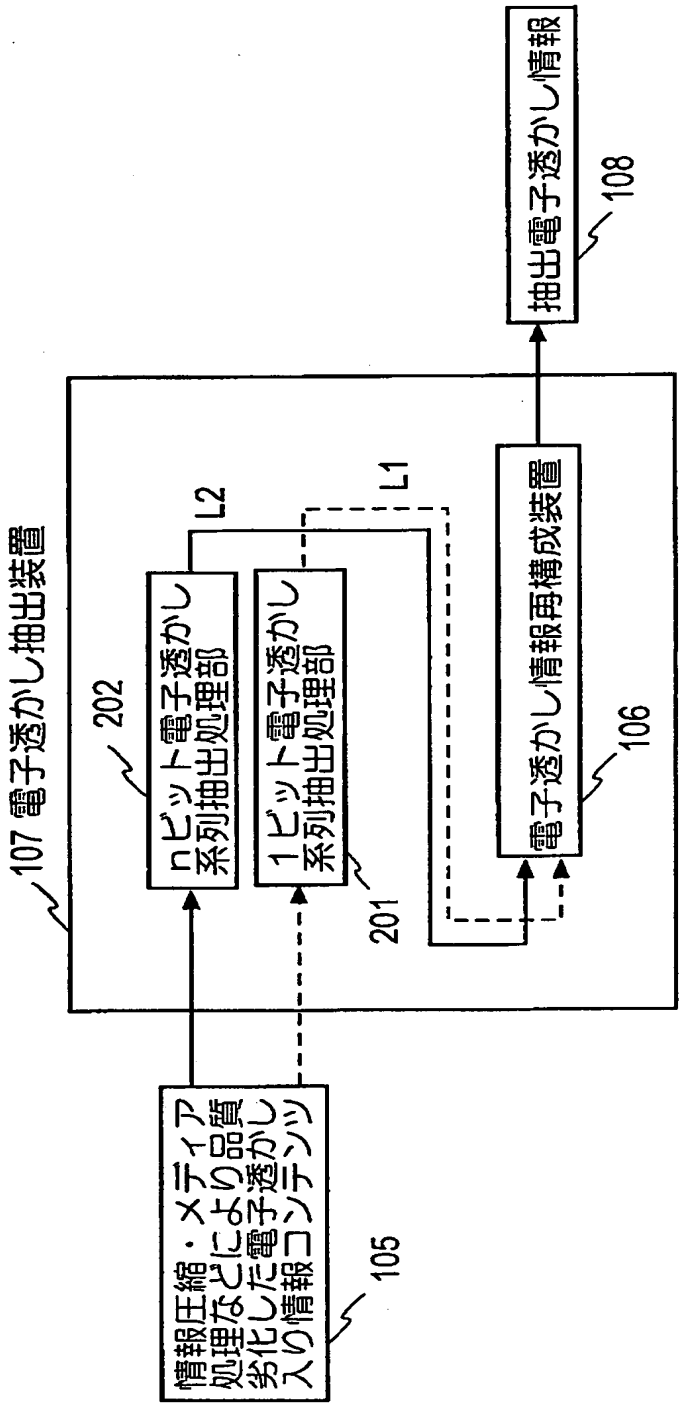
情報圧縮・メディア処理などにより劣化した電子透かし入り情報コンテンツ
105
107 電子透かし抽出装置
nビット電子透かし系列抽出処理部
202
1ビット電子透かし系列抽出処理部
201
L2
L1
電子透かし情報再構成装置
106
抽出電子透かし情報
108

図２

【図３】

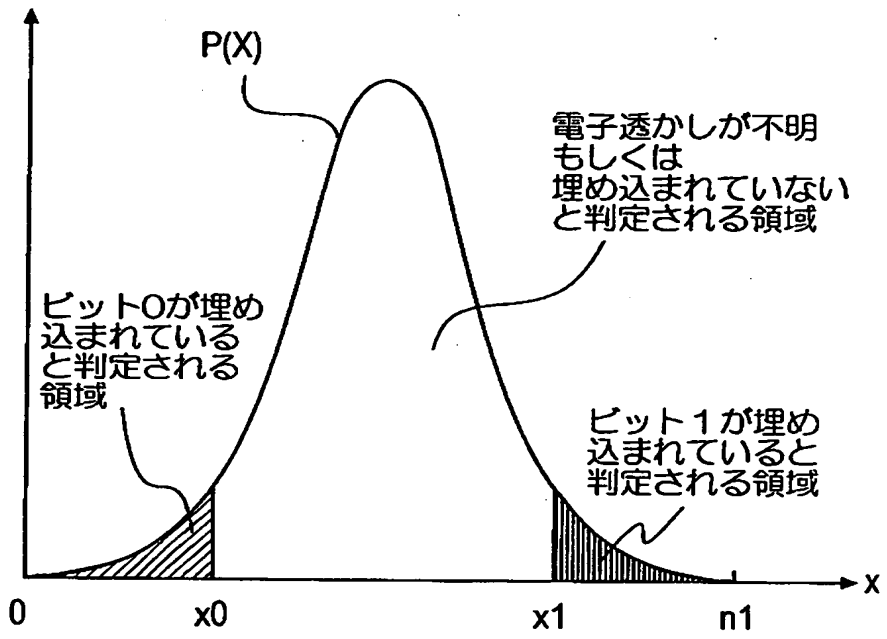
P(X)
電子透かしが不明
もしくは
埋め込まれていない
と判定される領域
ビットOが埋め
込まれている
と判定される
領域
ビット１が埋め
込まれていると
判定される領域
x
0
x0
x1
n1

図３

【図４】

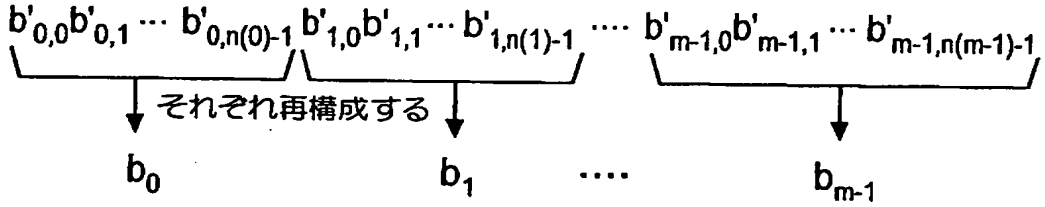
b'0,0b'0,1 … b'0,n(0)-1
b'1,0b'1,1 … b'1,n(1)-1
…. b'm-1,0b'm-1,1 … b'm-1,n(m-1)-1
それぞれ再構成する
b0
b1
….
bm-1

図４

【図５】

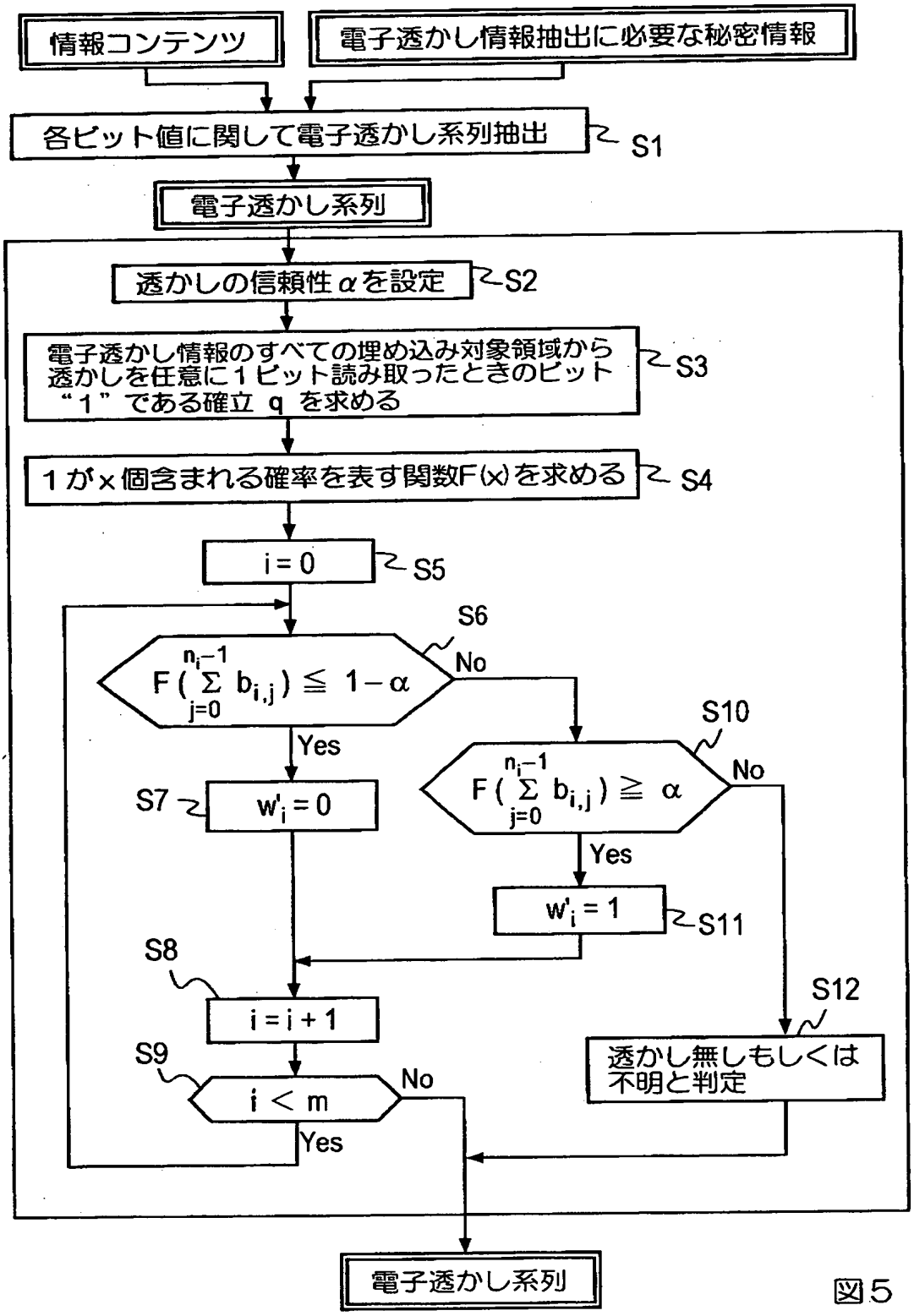
情報コンテンツ
電子透かし情報抽出に必要な秘密情報
各ビット値に関して電子透かし系列抽出
S1
電子透かし系列
透かしの信頼性αを設定
S2
電子透かし情報のすべての埋め込み対象領域から透かしを任意に１ビット読み取ったときのビット“１”である確立 q を求める
S3
１がｘ個含まれる確率を表す関数F(x)を求める
S4
i = 0
S5
S6
$F(\sum_{j=0}^{n_i-1} b_{i,j}) \leqq 1-\alpha$
No
Yes
S7
$w'_i = 0$
S10
$F(\sum_{j=0}^{n_i-1} b_{i,j}) \geqq \alpha$
No
Yes
$w'_i = 1$
S11
S8
i = i + 1
S9
i < m
No
Yes
S12
透かし無しもしくは不明と判定
電子透かし系列

図５

【図６】

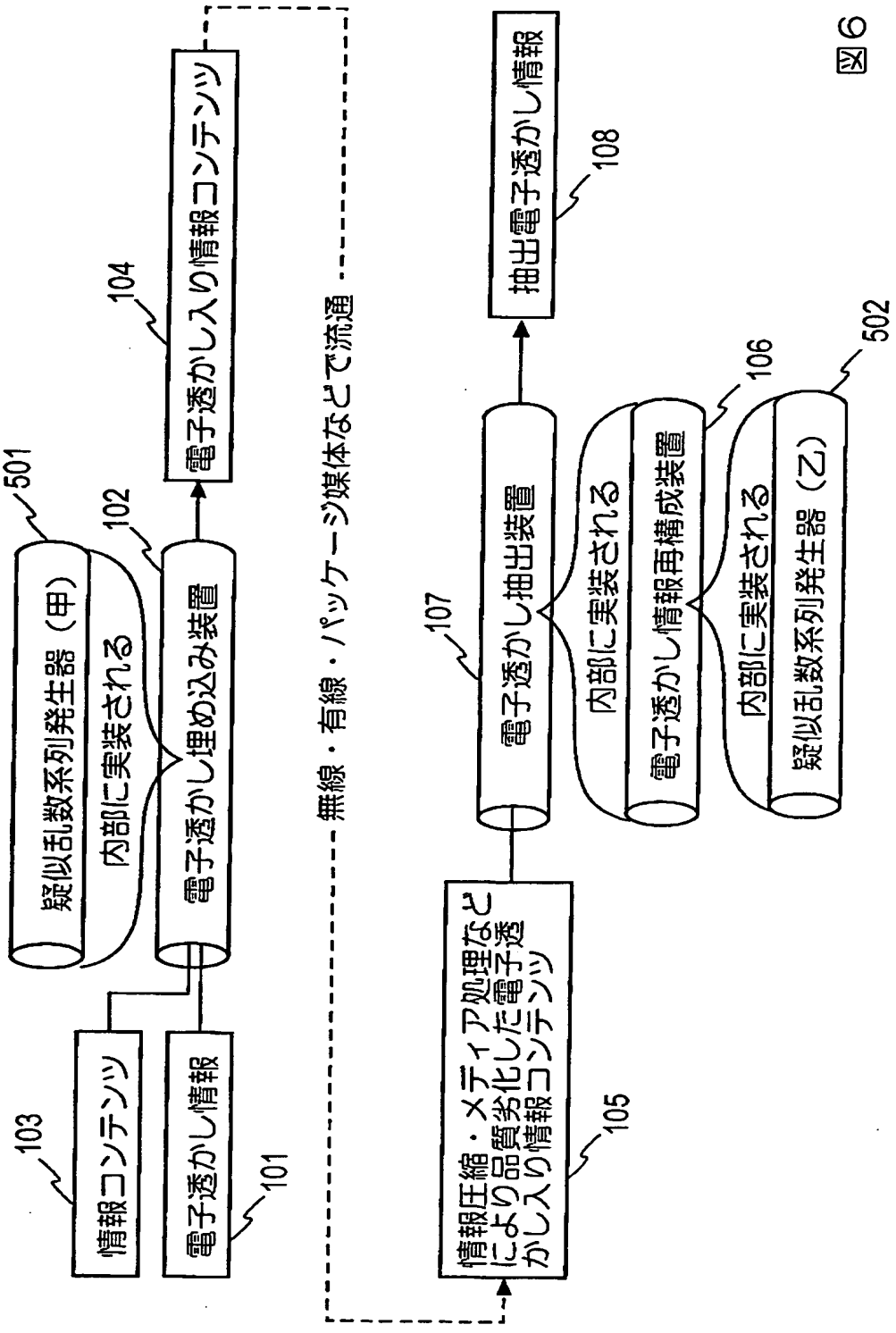
情報コンテンツ
103
電子透かし情報
101
電子透かし埋め込み装置
102
疑似乱数系列発生器（甲）
501
内部に実装される
電子透かし入り情報コンテンツ
104
無線・有線・パッケージ媒体などで流通
情報圧縮・メディア処理などにより品質劣化した電子透かし入り情報コンテンツ
105
電子透かし抽出装置
107
抽出電子透かし情報
108
内部に実装される
電子透かし情報再構成装置
106
内部に実装される
疑似乱数系列発生器（乙）
502

図６

【図７】

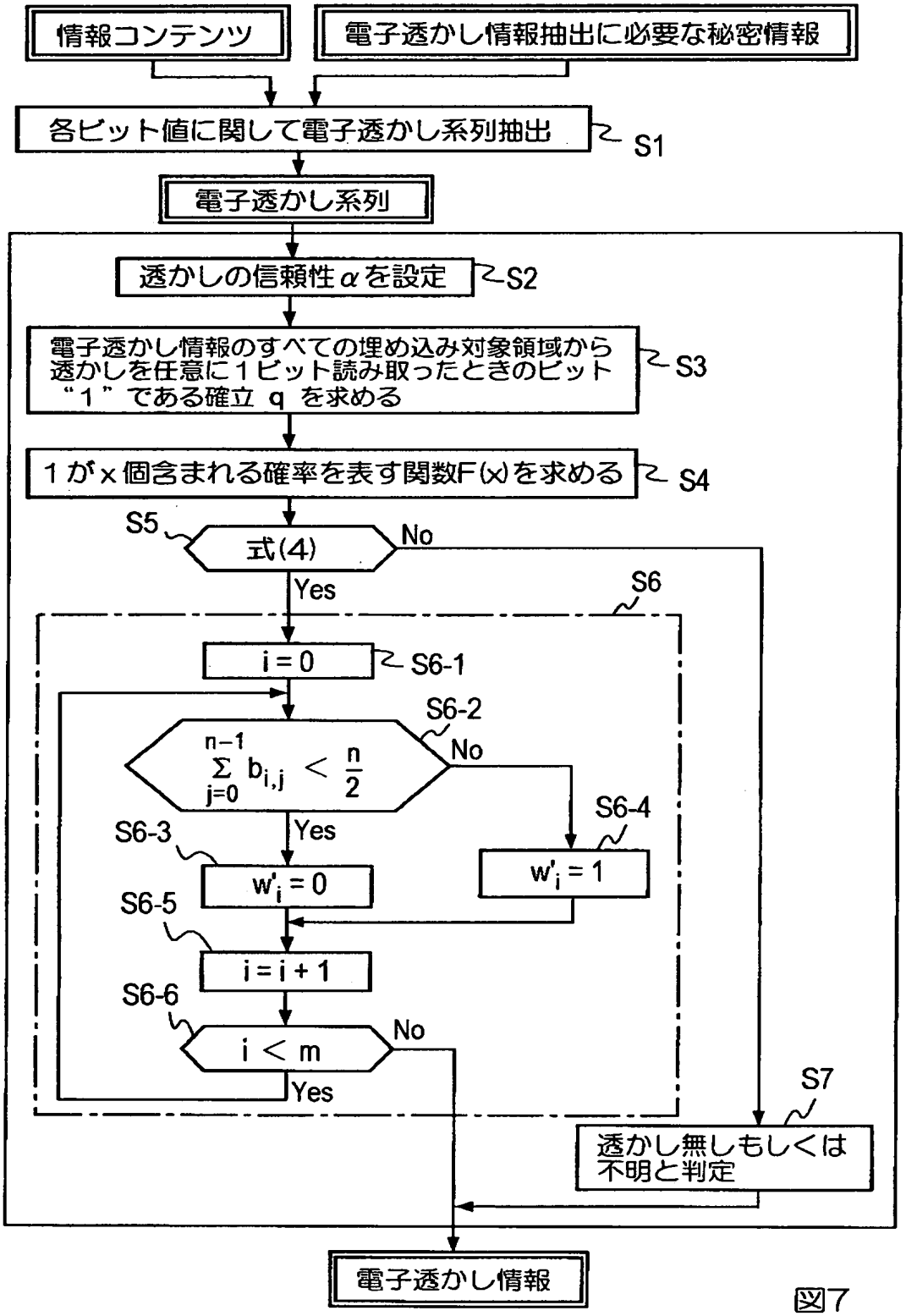
情報コンテンツ
電子透かし情報抽出に必要な秘密情報
各ビット値に関して電子透かし系列抽出
S1
電子透かし系列
透かしの信頼性αを設定
S2
電子透かし情報のすべての埋め込み対象領域から透かしを任意に１ビット読み取ったときのビット“１”である確立 q を求める
S3
１がｘ個含まれる確率を表す関数F(x)を求める
S4
S5
式(4)
No
Yes
S6
i = 0
S6-1
S6-2
$\sum_{j=0}^{n-1} b_{i,j} < \frac{n}{2}$
No
Yes
S6-3
S6-4
w'i = 0
w'i = 1
S6-5
i = i + 1
S6-6
i < m
No
Yes
S7
透かし無しもしくは不明と判定
電子透かし情報

図7

【図８】

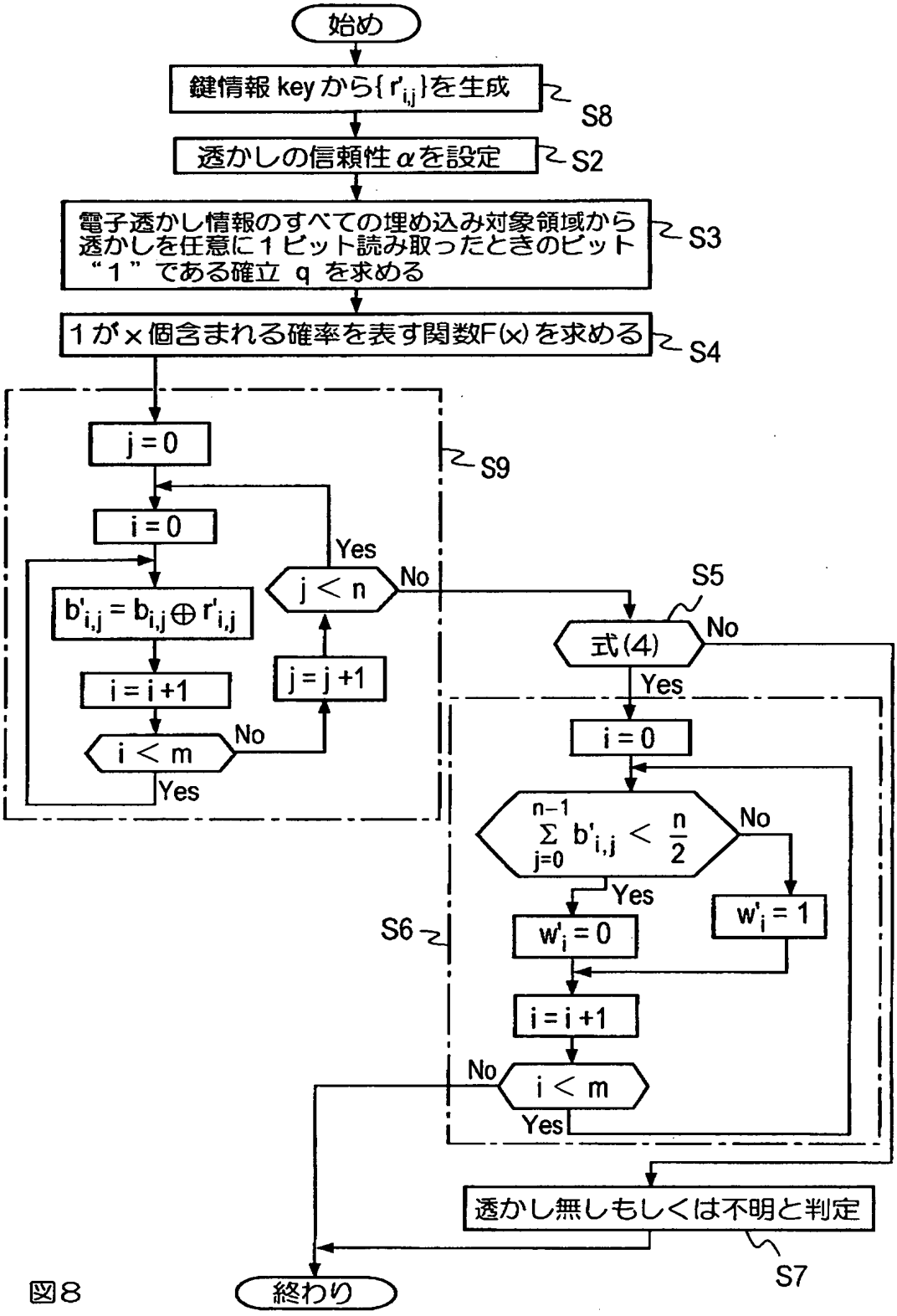
始め
鍵情報 key から{r'i,j}を生成
S8
透かしの信頼性αを設定
S2
電子透かし情報のすべての埋め込み対象領域から
透かしを任意に１ビット読み取ったときのビット
“１”である確立 q を求める
S3
１がｘ個含まれる確率を表す関数F(x)を求める
S4
S9
j = 0
i = 0
b'i,j = bi,j ⊕ r'i,j
i = i +1
i < m
No
Yes
j = j +1
j < n
No
Yes
S5
式(4)
No
Yes
i = 0
n-1 Σ b'i,j < n/2
j=0
No
Yes
S6
w'i = 0
w'i = 1
i = i +1
i < m
No
Yes
透かし無しもしくは不明と判定
S7
終わり

図８

【図９】

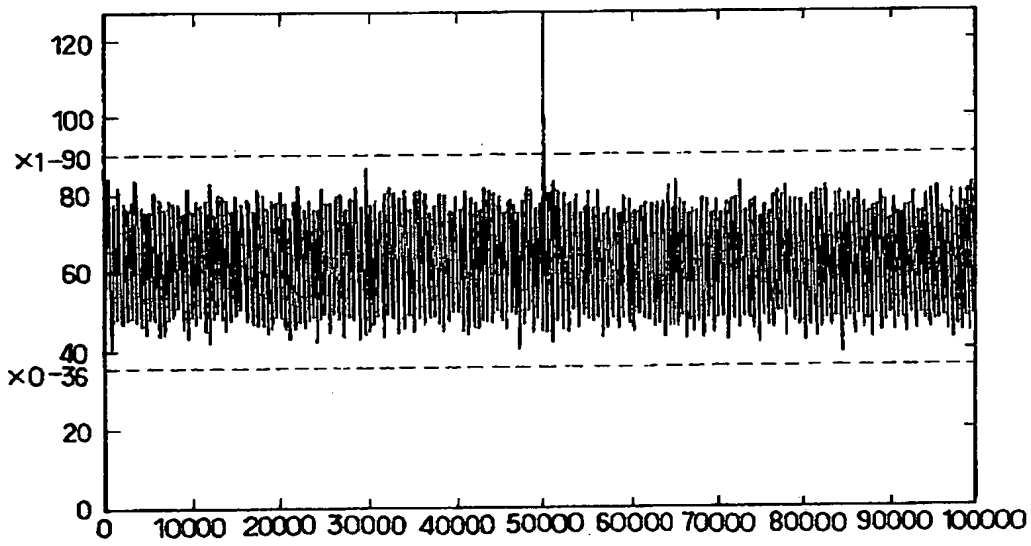
120
100
×1-90
80
60
40
×0-36
20
0
0
10000
20000
30000
40000
50000
60000
70000
80000
90000
100000

図9

【図１０】

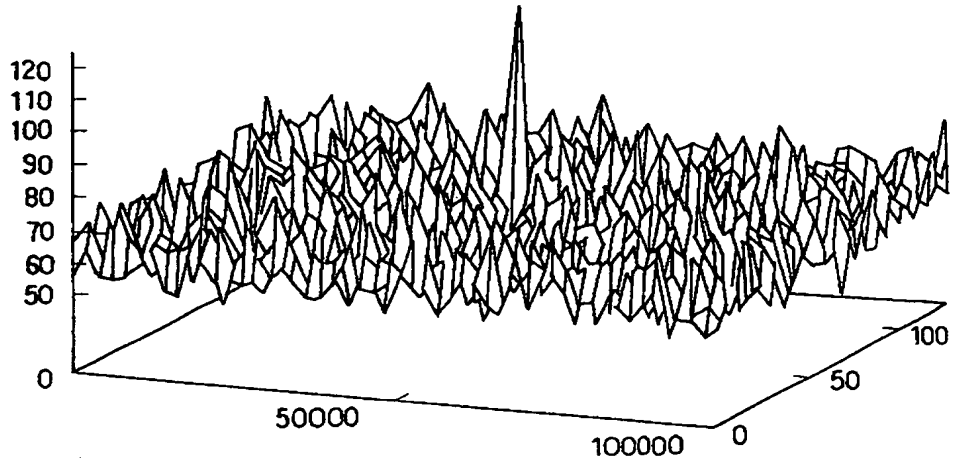
120
110
100
90
80
70
60
50
0
50000
100000
0
50
100

図10

【書類名】　　要約書

【要約】

【課題】　電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価する。

【解決手段】　情報コンテンツの透かし対象領域から無作為に１ビット透かし系列の抽出を行い、その時のビット０と１の出現確率１－ｑとｑを求め、透かしが埋め込まれたのべ回数n_iビットだけ透かし系列を抽出し、この時、n_iビット列に１がｋ個現れる確率

$$P(x=k)={}_{n_i}C_k\, q^k \cdot (1-q)^{ni-k}$$

その分布関数

$$F(x)=\sum_{k=0}^{x} {}_{n_i}C_k\, q^k \cdot (1-q)^{ni-k} \quad (0\leq x\leq n_i)$$

より、透かし情報の信頼度のしきい値α（１／２＜α≦１）に対し、$0\leq F(x=x_0)\leq 1-\alpha$を満す最大の$x_0$と、$\alpha\leq F(x=x_1)\leq 1$を満す最小の$x_1$をそれぞれ透かし情報判定しきい値とする。

【選択図】　　図３

認定・付加情報

特許出願の番号	平成１１年　特許願　第１１８０７２号
受付番号	５９９００４００２７３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１１年　５月　６日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000004226
【住所又は居所】	東京都新宿区西新宿三丁目１９番２号
【氏名又は名称】	日本電信電話株式会社

【代理人】　申請人

【識別番号】	100066153
【住所又は居所】	東京都新宿区新宿四丁目２番２１号　相模ビル
【氏名又は名称】	草野　卓

【選任した代理人】

【識別番号】	100100642
【住所又は居所】	東京都新宿区新宿４丁目２番２１号　相模ビル 草野特許事務所
【氏名又は名称】	稲垣　稔

次頁無

出証特平１１－３０６０１０５

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９５年　９月２１日
［変更理由］　住所変更
住　所　東京都新宿区西新宿三丁目１９番２号
氏　名　日本電信電話株式会社

２．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社